A CYBER FORENSICS STUDY OF ATM DATA TRAFFIC

Dr.Egho-Promise Ehigiator Iyobor,
Regional Technical Head, Glo Mobile Ghana Limited, Tamale,
Northern Region, Ghana
eghopromise@yahoo.com

Bamidele Ola,
Technobeacon Consulting Ltd,
London, United Kingdom

Emmanuel Opoku Sarkodie
Managing Partner, Lyonsark Creation, Accra,
Greater Accra, Ghana

Publication History
Manuscript Reference No: IJIRIS/RS/Vol.07/Issue07/AUIS10080
Received: 03, August 2020
Accepted: 20, August 2020
Published Online: 22, August 2020
DOI: https://doi.org/10.26562/ijiris.2020.v0707.001
https://doi.org/10.26562/ijiris.2020.v0706.001
Peer-review: Double-blind Peer-reviewed
Editor: Dr.A.Arun L.S, Chief Editor, IJIRIS, AM Publications, India
Copyright: ©2020 This is an open access article distributed under the terms of the Creative Commons Attribution License; Which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited

Abstract: For several years now, bank customers have become accustomed to the convenient use of Automated Teller Machines (ATM) to transfer money between accounts either within the same bank or to different banks. The ATM provides account balance information, enable customers to deposit and withdraw cash from their accounts and perform other transactions without physically meeting bank staff in banking hall for transactions. The use of ATMs for mobile banking has led to a significant increase in ATM fraud globally. Consumer confidence in the use of ATMs for banks transactions and credit card issuers has been impacted by fraudulent activities associated with ATMs.

Keywords: data; Study; cyber; forensics, ATM

1. INTRODUCTION

Automated Teller Machine (ATM) is electronic equipment which allows bank customers to perform some transactions either within or outside banking premises. Such transactions include: withdrawals, deposits, checking account balances, transferring of money within the same or different banks, paying utilities bills, to mention but a few. ATM facilitates a convenient method for customers to execute banking transactions and invariably provides avenues for committing cybercrime in cyberspace. Cyber forensics is a branch of computer science that deals with how to obtain, preserve, analyze, document and present digital data from cyber space. A cyber forensics investigator or cyber forensics analyst is a professional or expert who obtain digital data from cyberspace, perform analysis and documents evidential data, which can be admissible in the law courts. When cybercrime is committed in ATM transactions, forensic experts are required to investigate and extract digital data from the cyberspace where the crime was committed with the aid of forensic tools. Using the ATM digital data traffic collected, the forensic expert conducts a forensic analysis of the ATM digital data traffic, preserves the integrity of the data, prepares a report which can be admissible in the court of law. Assets stolen can be recovered through Alternative Dispute Resolution (ADR) or through adjudication of law courts.

1.1 Problem Statement

Financial institutions and individual’s lose substantial amount of money from ATM fraud.

1.2 Significance of the problem

The study will enable the network cyber forensics investigator to extract digital evidence from the generated data packets from ATM networks. The investigator will be able to perform analysis on the data in a forensic laboratory and prepare a report that can be presented in the court of law to enable recovery of stolen assets.

1.3 Objectives

The objectives of the study include:
1. To capture data traffic generated from ATM networks
2. To provide digital evidence in court of law in case cybercrime is committed
3. To recover stolen money for individual or financial institutions
II. LITERATURE REVIEW

The first ATM came into existence in 1967 at Barclays bank branch in London, although it was reported that Japan started using cash dispenser in mid-1960s but the ATM network communication between different banks started later in 1970. The concept of ATM has been existing for nearly 20 years but we have recently seen a sharp increase in popularity and integration into the entire security infrastructure [12][15]. ATM is also known as Alternative Delivery Channel because it is a substitute for the manual teller. It is a channel also because in the banking world, all delivery mechanisms require a delivery channel [11]. ATM fraud has increased suddenly and unexpectedly at the highest rate in two decades according to [17]. The rise in ATM fraud cases is mainly due to the use of credit and debit cards launched by competing banks and credit card companies to replace the 30-year-old magnetic stripe technology. ATM fraud does not only cause financial losses to banks but also undermines customer’s confidence in the use of ATM for financial transactions [5].

ATM network is vulnerable to different attacks which is similar to those of IP based networks. Attacks are often carried out remotely by cybercriminals such attacks include Denial of Service (DoS), packet sniffing, theft of virtual channel by criminal organization [6]. Criminals do take advantage of ATM vulnerabilities and exploit these loopholes for committing various cybercrimes. The threat to ATMs is not only a local threat to one computer, but it can also be found in cloud services that provide identity verification and transaction information between ATMs, card holders, and the processing agent infrastructure. “With the introduction of internet technology in recent years, cyber criminals take advantage of the ATM vulnerabilities and perform attacks on ATM systems” [20]. In this statement, you can discover and support the importance of this research. With the major shift from plain old telephone service (POTS) [13] as a primary method of communication to Ethernet-based technology, a medium has been opened to capture transaction data and allow criminals to raid ATM machines, customer accounts, and consumer trust in banks and credit card companies. Around the world, about $45 million was announced to have been stolen through ATM [12]. The scale of the impact on consumer confidence is a frequently studied phenomenon in many countries around the world. This provides an incentive to assess security risks, develop standards, and create standards to discover and evaluate affected aspects of ATM transactions more effectively and clearly. The security and privacy of customers information (PIN codes, passwords, etc.) is a major pressing issue that affect customer satisfaction and dissatisfaction [10][14]. The various literature reviewed revealed only security vulnerabilities of ATMs [2][8][15][16][22][23], cybercrimes associated with ATM [1][10][18][20], and its effect on the users [3][5][10] but there has not been research work on ATM data traffic for cyber forensics analysis and the methods of recovery stolen assets. This study will bridge these gaps in the literature.

2.1 Types of ATM

ATM is classified into two main categories:

i. Simple ATM: This type of ATM allows bank customers to perform simple transactions such as withdrawing of cash and checking accounts balance

ii. Complex ATM: This ATM enables customers of the banks to carry out so many transactions such as cash withdrawal, deposit, inter and intra bank transfer, check accounts balance, pay bills, etc

2.2 Components of ATM

Every ATM comprises of the following components:

i. Display Unit: every transaction carried out by customers are displayed on the display unit such as Liquid Crystal Display, Visual Display Unit, etc.

ii. Printer: it prints receipts of transactions performed by customers

iii. Cash Dispenser: the ATM has a slot that dispenses money

iv. Keypad: it is an input device that allows customers to enter data into the system. Such data include Personal Identification Number (PIN), kind of transactions, amount, etc.

v. Card Reader: it displays customers account information and instructions on how to perform different transactions

2.3 ATM Operations

Figures 1 and 2 below represent ATM network and flowchart showing ATM transactions. The ATM network comprises of bank computer, host computer and ATM as well as transmission links or media provided by Internet Service Provider (ISP). The ISP offers internet services between ATM and the host processors (server).

Figure 1: ATM Network
Any data entered into ATM by the cardholders is transferred to the server. The processor validates the data with an authorized bank. The host processor sends endorsement code to the ATM so that the money can be dispensed.

### 2.4 Benefits of ATM

- **i.** It provides convenience for customers of the banks
- **ii.** It decreases the workload of bank staff
- **iii.** It provides 24/7 hours services

### 2.5 Packet Sniffing

Packet sniffing also referred as network protocol analysis is a method of monitoring and collecting network data packets passing through computing networks using tools called packet sniffers [7]. Examples of sniffing tools are Wireshark®, Ettercap®, BetterCap®, TCPDump®, WinDump®. A network administrator uses the tool to keep track of data traffic on the network, manage network bandwidth and manage network security. Sniffing in the wrong hands is harmful to users and networks since hackers can sniff email traffic, web traffic, file transfer protocol (FTP) session passwords, telnet session passwords, chat sessions, and domain name system (DNS) traffic to commit cybercrime [7].

The data traffic captured by the packet sniffer can also be used by cyber forensics in case cybercrime is committed in the ATM network for legal purposes. The cyber forensics investigator extracts these digital data, perform analyses and documentations of the data in forensics lab and present the report in the court of law. The investigator also ensures the preservation of the integrity of the digital data. In this study, a Wire-shark sniffing tool [4][21] was used and not firewall [9] because it is freely and readily available and can help to discover malicious activities in the ATM network besides identification of dropped packets, detecting the root cause of network issues and resolving latency problems.

### III. METHODOLOGY

Quantitative research approach and experimental research method were adopted in this study. The method allows for observation and collection of data traffic on real time basis.

---

**Figure 2: Flowchart showing ATM transactions**

---
3.1 Data collection
As shown in Figure 3, the packet sniffing host is connected to the hub to provide access to all data traffic on the ATM network. Every data that passes through a hub is received by the packet sniffing host.

![Figure 3: ATM Network with few network devices showing how data traffic is captured by packet sniffer](image)

The packet sniffing host is connected to the hub in a larger network to gain access to data traffic on the ATM network.

3.2 Hardware and software
The hardware and software tools below were used in the study:
- Microsoft® Windows® 10 operating system
- Computer systems
- Wireshark® Network Analyzer v2.6.4
- Hubs
- Routers
- Switches
- Credit cards.

IV. DATA ANALYSIS AND EXPERIMENTAL RESULTS
Figure 5 below shows the experimental results of data captured by packet sniffer in the ATM networks. After confirming that the ATM has passed the authentication of the processing server, a test transaction is performed. The figure displayed authentication to the server (host processor) with IP address of 206.71.17.21 and the ATM address of 192.168.0.7. Once the ATM receives DHCP services and dynamically obtains the assigned IP addresses, it will collect data traffic that shows the IP addresses. Then, the ATM is statically configured to have the same dedicated IP address to keep the data collected consistently and efficiently [19].

![Figure 4: ATM Network with several network devices indicating how data traffic is collected by packet sniffer in a large network](image)
Both figures 5 and 6 showed changes in the conditions of the network infrastructure between the ATM and the processing server, which requires re-transmission of the packet or repeated confirmation. Figure 7 also displayed packets overhead.
Both figures 7a and 7b showed password verification, successful operations and failed transactions suspected to be malicious activities, etc.
V. CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusion
We have captured ATM data traffic using packet sniffer with Wireshark application. The adopted procedures successfully collected adequate data from both small and larger networks as experimented above and these data can be used by a cyber forensics investigator to carry out data analyses and documentations for legal purposes in order to recover stolen money by cybercriminals.

5.2 Recommendations
It is recommended that a cyber forensics investigator should have adequate ATM data traffic for effective and efficient digital data analyses and reporting in case cybercrime is committed in the ATN network. This report can be presented in the court of law or used in case Alternative Dispute Resolution (ADR) approach is applied to resolve the issues.

REFERENCES